Configuring VRRP Services

BayRS Version 13.10
Site Manager Software Version 7.10

Part No. 304138-A Rev 00
November 1998

Bay Networks *Where Information Flows.*™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. November 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, Switch Node, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these

terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. (“Bay Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT

SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin ix
Text Conventions x
Acronyms xi
Bay Networks Technical Publications xi
How to Get Help xii

Chapter 1
VRRP Concepts

About VRRP 1-1
Master Virtual Router 1-2
Backup Virtual Routers 1-2
Critical IP Interfaces 1-2
VRRP Messaging 1-2
Planning Your Network 1-3
Sample Configurations 1-3

Chapter 2
Starting VRRP Services Using Site Manager

Configuring a Virtual Router 2-1

Chapter 3
Customizing VRRP

Disabling and Reenabling a Virtual Router 3-2
Changing the IP Address Backed Up by a Virtual Router 3-3
Setting the Priority of the Virtual Router 3-4
Setting the Advertisement Interval 3-5
Setting the Critical IP Interface Address 3-6
Setting the Token Ring Address 3-7

Appendix A Site Manager Parameters

Add Virtual Router Parameters A-1
VRRP Configuration Parameters A-3

Glossary

Index

Figures

Figure 1-1. Using VRRP with One Master and One Backup Virtual Router 1-3
Figure 1-2. Using VRRP and Perfoming Load-Balancing 1-4
Figure 1-3. Using VRRP with a Critical IP Interface 1-5
Figure 1-4. Sample Invalid Virtual Router Configuration 1-6
Figure A-1. Add Virtual Router Window A-1
Figure A-2. IP VRRP Configuration Parameters Window A-3

Preface

This guide describes the Virtual Router Redundancy Protocol (VRRP) and what you do to start and customize VRRP services on a Bay Networks® router.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

bold text	Indicates text that you need to enter and command names and options. Example: Enter **show ip** {**alerts** | **routes**} Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

IP	Internet Protocol
LAN	local area network
MAC	media access control
MIB	management information base
VRID	virtual router ID
VRRP	Virtual Router Redundancy Protocol

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
VRRP Concepts

This chapter describes VRRP concepts you need to know before you begin configuring a VRRP router.

Topic	Page
About VRRP	1-1
Master Virtual Router	1-2
Backup Virtual Routers	1-2
Critical IP Interfaces	1-2
VRRP Messaging	1-2
Planning Your Network	1-3

About VRRP

The Virtual Router Redundancy Protocol (VRRP), which runs over IP, enables you to configure router redundancy to protect a network from the irrecoverable failure of one or more IP interfaces. VRRP manages a virtual router, which is a software-defined object that corresponds to an IP address on a LAN segment. A virtual router typically exists on multiple routers running VRRP (known as VRRP routers). One of the VRRP routers acts as the master virtual router for an IP address, while other VRRP routers act as backup virtual routers.

You identify each virtual router using a virtual router identifier (VRID) and a virtual router IP address. All VRRP routers on a LAN segment must have the same VRID and IP address. You can, however, use a VRID on more than one LAN as long as you pair it with a different virtual router IP address. The scope of each virtual router is restricted to a single LAN.

Master Virtual Router

The master virtual router is the VRRP router responsible for forwarding the traffic received at the MAC address associated with the virtual router IP address. A VRRP router with the highest priority assumes the responsibilities of the master virtual router. When the master virtual router fails, one of the backup virtual routers becomes the master virtual router.

Backup Virtual Routers

If the master virtual router becomes unavailable or if it is not functioning normally, VRRP dynamically switches over to one of the backup virtual routers, in the order of the priority you set.

If more than one backup virtual router has the same priority assigned to it, the VRRP router with the greater primary IP address will become the new master virtual router.

Critical IP Interfaces

You can establish a critical IP address, which is a physical IP interface on a local router, for each virtual router. If that critical IP interface fails, then VRRP switches to another virtual router. Figure 1-3 on page 1-5 shows a sample VRRP configuration using a critical IP interface.

VRRP Messaging

VRRP generates VRRP advertisement messages as IP multicast datagrams, enabling VRRP to operate over a variety of multiaccess LAN technologies that support IP multicasting.

Planning Your Network

You can use VRRP to target stub networks with hosts having default gateway addresses to provide redundancy for IP addresses. To avoid a single point of failure, you should configure the default gateway IP address as the virtual router IP address on multiple IP interfaces on different physical routers. Refer to the following sample configurations when determining how to configure VRRP in your network.

Sample Configurations

The configuration in Figure 1-1 shows a simple VRRP scenario in which both router A and router B are running VRRP. The end hosts install a default route to the IP address of router A, which serves as the master virtual router for virtual router 1. If router A fails, then router B becomes the master virtual router for virtual router 1.

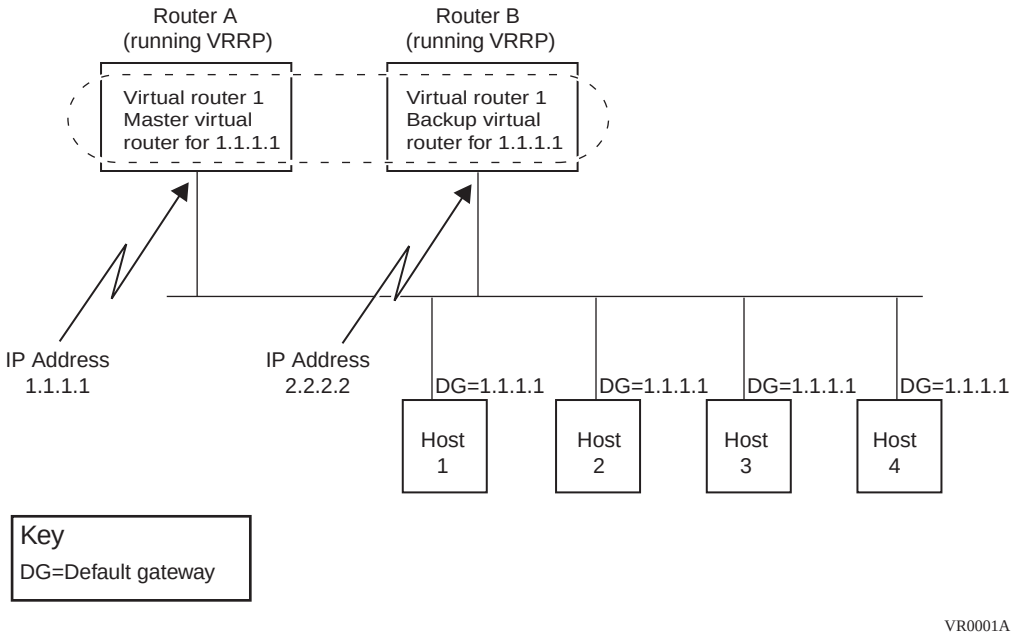

Figure 1-1. Using VRRP with One Master and One Backup Virtual Router

The configuration in Figure 1-2 shows that half of the hosts install a default route to VRRP router A's IP address (1.1.1.1), and the other half install a default route to VRRP router B's IP address (2.2.2.2). Using two different default routes has the effect of load-balancing the outgoing traffic, while also providing full redundancy.

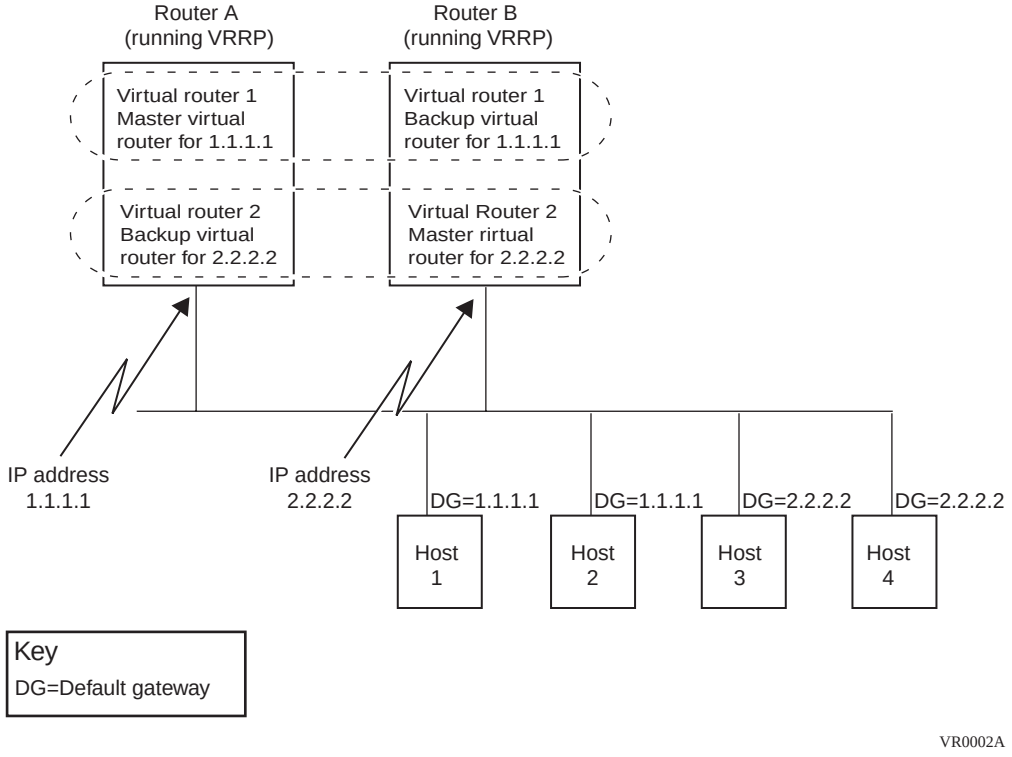

Figure 1-2. Using VRRP and Perfoming Load-Balancing

The configuration in Figure 1-3 shows that IP address 1.1.1.1 provides connectivity to external networks. If that connection fails and the virtual router 1 on router B continues to forward traffic, you still lose connectivity to external networks. However, if you designate IP address 1.1.1.1 as the critical IP address for virtual router 1 on router B, and IP address 1.1.1.1 fails, then virtual router 1 on router A becomes the master virtual router and begins forwarding traffic.

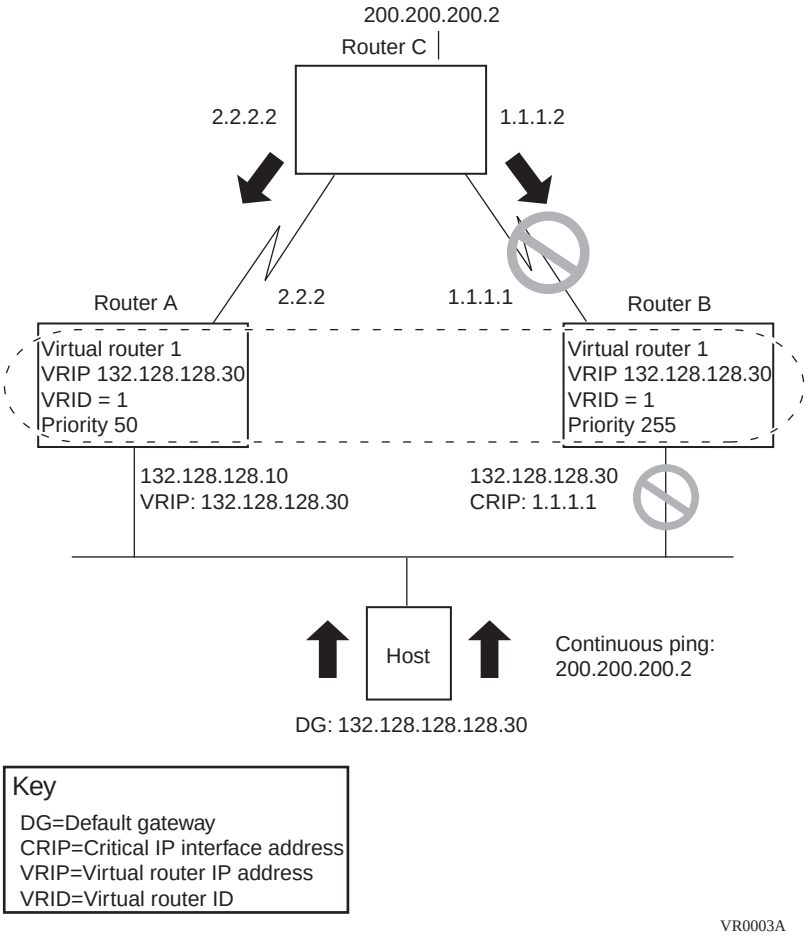

Figure 1-3. Using VRRP with a Critical IP Interface

Figure 1-4 shows an invalid VRRP configuration; that is, the virtual router with primary IP address 1.1.1.1 is not configured on a VRRP router that has a physical interface with IP address 1.1.1.1. You must always configure a virtual router whose IP address physically exists on the LAN. For example, you must configure virtual router 1 on router A, because the IP address of virtual router 1 is the same as the physical address of router A.

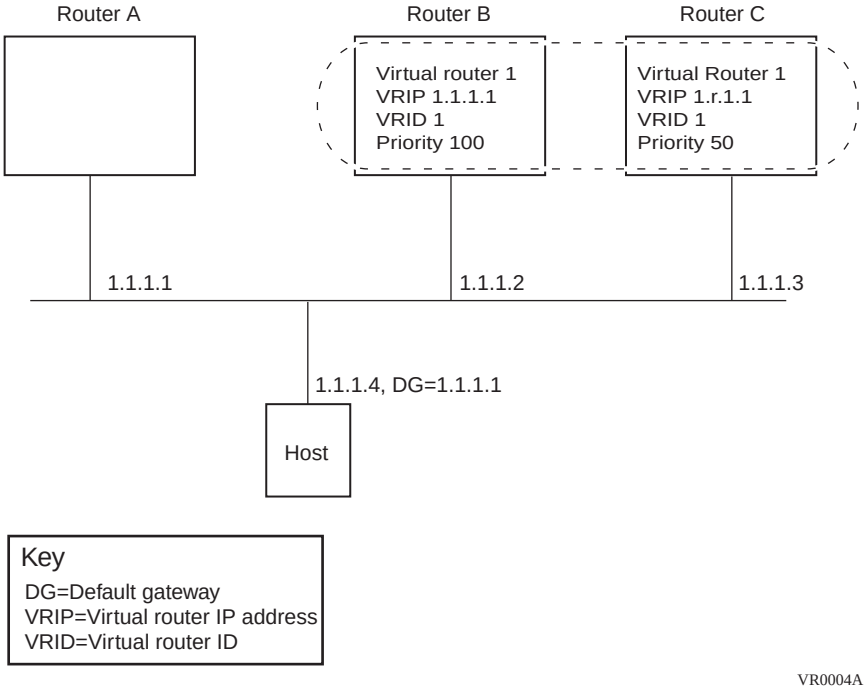

Figure 1-4. Sample Invalid Virtual Router Configuration

Chapter 2
Starting VRRP Services Using Site Manager

You must configure IP services on a router before you can configure VRRP. See *Configuring IP Services* for information about how to configure IP.

You can create a basic virtual router configuration by supplying only the required configuration information and accepting the default values for all other Site Manager parameters.

Configuring a Virtual Router

When configuring a virtual router, you must supply the following:

- Primary IP address

  The primary IP address associates a virtual router with the IP address of the physical interface. You cannot change the primary IP address after you configure a virtual router. If this primary IP address matches the virtual router IP address and the virtual router has the highest priority of 255, then this VRRP router becomes the master virtual router, if it is available.

Caution: You should not configure an Ethernet interface as the master virtual router on an ANH™ router.

- Virtual router ID

  The virtual router ID (VRID) identifies the virtual router. VRRP uses the virtual router ID to calculate the virtual router's virtual MAC address. If the virtual router is in the primary virtual router state, it responds to all ARP requests using the IP address of the virtual router with its virtual MAC address, not its physical MAC address. You cannot change the virtual router ID after you configure a virtual router.

- Virtual router IP address

  The virtual router IP address identifies the IP address that the virtual router backs up.

To configure a virtual router, complete the following tasks:

Caution: If you are configuring virtual routers on the IP interface used as the Site Manager management console, you should not add or modify a backup virtual router before you create a master virtual router. Otherwise, you can lose connectivity to the router when dynamically configuring virtual routers. Use local or remote mode when configuring a virtual router.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on **Add**.	The Add Virtual Router window opens.
5. Set the following parameters: • **Primary IP Address** • **Virtual Router ID** • **Virtual Router IP Address** Click on **Help** or see the parameter descriptions starting on page A-2.	
6. Click on **OK**.	You return to the Configuration Manager window.

Chapter 3
Customizing VRRP

To customize VRRP, use the information in the following sections

Topic	Page
Disabling and Reenabling a Virtual Router	3-2
Changing the IP Address Backed Up by a Virtual Router	3-3
Setting the Priority of the Virtual Router	3-4
Setting the Advertisement Interval	3-5
Setting the Critical IP Interface Address	3-6
Setting the Token Ring Address	3-7

Caution: If you are configuring virtual routers on the IP interface used as the Site Manager management console, you should not add or modify a backup virtual router before you create a master virtual router. Otherwise, you can lose connectivity to the router when dynamically configuring virtual routers. Use local or remote mode when configuring a virtual router.

Disabling and Reenabling a Virtual Router

When you first configure a virtual router, by default Site Manager enables that virtual router. To disable or reenable a virtual router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Changing the IP Address Backed Up by a Virtual Router

When you first configure a virtual router, you must supply an IP address that the virtual router backs up. This IP address must be on the same subnet as the primary IP address.

To change the IP address to be backed up by a virtual router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.
5. Set the **Virtual Router IP Address** parameter. Click on **Help** or see the parameter descriptions starting on page A-4.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Priority of the Virtual Router

You can set the priority of the virtual router in relation to all virtual routers that have the same virtual router ID and are on the same subnet. The higher you set the value, the higher the priority of the virtual router.

When you initially configure a virtual router, if the primary IP address is the same as the virtual router IP address, Site Manager automatically sets the priority to the highest priority (255) and the virtual router becomes the master virtual router as soon as it comes up. If you initially configure a backup virtual router and later change the primary IP address to the virtual router IP address, you must manually change the priority to 255 for the virtual router to become the master virtual router.

By default, Site Manager assigns a priority of 100 to all backup virtual routers. You can set the priority for backup virtual routers from 1 to 254. If you assign more than one backup virtual router the same priority, the VRRP router with the greater primary IP address takes precedence.

To set a virtual router's priority, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted virtual router appears.
5. Set the **Priority** parameter. Click on **Help** or see the parameter descriptions starting on page A-4.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Advertisement Interval

The advertisement interval determines the interval, in seconds, between transmissions of VRRP advertisements from the master virtual router to notify all backup routers that it is currently the master virtual router and is forwarding all traffic. You must set the same advertisement interval for all VRRP routers having the same VRID on the same LAN.

To set the advertisement interval, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **Advertisement Interval** parameter. Click on **Help** or see the parameter descriptions starting on page A-4.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Critical IP Interface Address

The critical IP interface resides on the same router as a physical interface. The state of the critical IP interface determines the state of the virtual router. If the critical interface fails, the virtual router fails and the VRRP router with the next highest priority becomes the master virtual router and begins routing traffic to its destination.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **Critical IP Interface** parameter. Click on **Help** or see the parameter descriptions starting on page A-5.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Setting the Token Ring Address

If you are running VRRP on a token ring network, VRRP uses the token ring functional address you provide instead of a virtual router MAC address. The token ring address identifies the token ring functional address for the virtual router MAC address that is configured on an IP interface over token ring.

Caution: For all virtual routers running over token ring, you must supply token ring functional addresses for virtual router MAC addresses or VRRP will fail.

To set the token ring address, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **VRRP**.	The IP VRRP Configuration Parameters window opens.
4. Click on a virtual router instance ID to highlight it in the list of virtual routers.	The configuration that pertains to the highlighted router appears.
5. Set the **Token Ring Address** parameter. Click on **Help** or see the parameter descriptions starting on page A-5.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

Appendix A Site Manager Parameters

This appendix explains all VRRP parameters and how to use them to customize a virtual router that you have added to an IP interface.

Add Virtual Router Parameters

The VRRP parameters displayed in the Add Virtual Router window (Figure A-1) enable you to establish a virtual router on an IP interface.

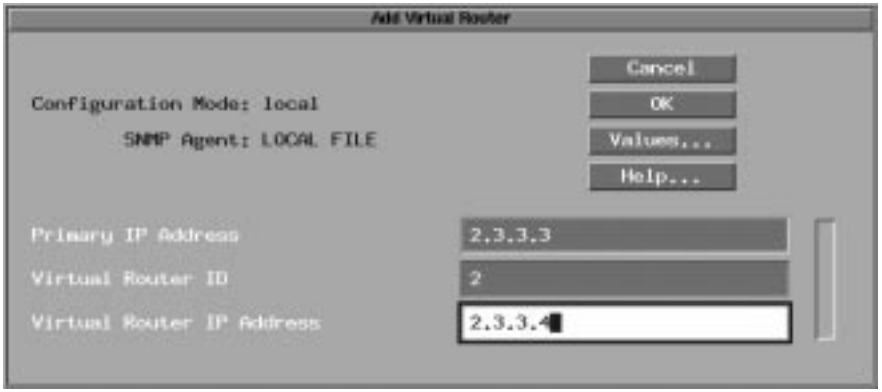

Figure A-1. Add Virtual Router Window

Parameter: Primary IP Address

Path:	Configuration Manager > Select Protocols > IP > VRRP > Add
Default:	None
Options:	Any valid IP address in dotted-decimal notation.
Function:	Identifies the IP address of the physical interface. The router lists this IP address as the source in VRRP advertisements sent by the virtual router.
Instructions:	Ensure that the primary IP address and the virtual router IP address are on the same subnet.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.4

Parameter: Virtual Router ID

Path:	Configuration Manager > Select Protocols > IP > VRRP > Add
Default:	None
Options:	1 to 255
Function:	Identifies the virtual router's ID (VRID). The router uses this number to calculate the MAC address. The VRID must be unique on the LAN segment.
Instructions:	Enter the ID of the virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.5

Parameter: Virtual Router IP Address

Path:	Configuration Manager > Select Protocols > IP > VRRP > Add
Default:	None
Options:	Any valid IP address in dotted-decimal notation.
Function:	Identifies the IP address that the virtual router backs up.
Instructions:	Ensure that the primary IP address and the virtual router IP address are on the same subnet. If the virtual router IP address is the same as the primary IP address, then this VRRP router, when operating, will always be the master virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.6

VRRP Configuration Parameters

The VRRP configuration parameters enable you to customize a virtual router. You access these parameters from the IP VRRP Configuration Parameters window (Figure A-2).

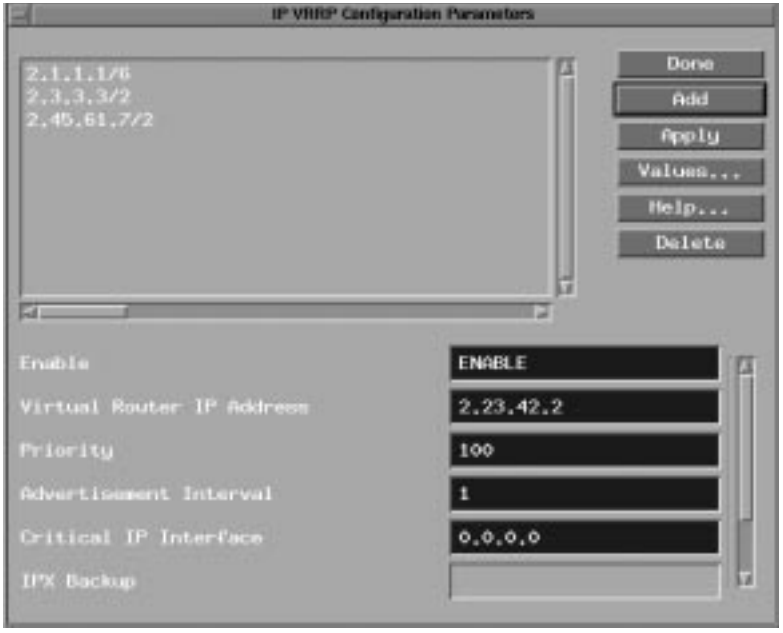

Figure A-2. IP VRRP Configuration Parameters Window

Parameter: Enable

Path: Configuration Manager > Select Protocols > IP > VRRP

Default: Enable

Options: Enable | Disable

Function: Enables or disables a virtual router on an interface.

Instructions: Select Enable to Enable a virtual router on an interface. Select Disable to disable a virtual router on an interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.25.1.1.2

Parameter: Virtual RouterIP Address

Path:	Configuration Manager > Select Protocols > IP > VRRP
Default:	None
Options:	Any valid IP address in dotted-decimal notation.
Function:	Identifies the IP address of the interface that the virtual router backs up.
Instructions:	Enter the IP address that you want the virtual router to back up. Ensure that the primary IP address and the virtual router IP address are on the same subnet. If the virtual router IP address is the same as the primary IP address, you should set the priority to 255 and then this VRRP router, when operating, will always be the master virtual router.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.6

Parameter: Priority

Path:	Configuration Manager > Select Protocols > IP > VRRP
Default:	100
Options:	1 to 255
Function:	Specifies the priority of the virtual router with respect to all virtual routers on the IP interface.
Instructions:	Enter a priority from 1 to 254. The higher the value you specify, the higher the priority of the virtual router. Site Manager automatically supplies a priority of 100 for all backup virtual routers. If you set the primary IP address to the IP address of the physical interface, Site Manager sets the priority to 255.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.25.1.1.8

Parameter: Advertisement Interval

Path:	Configuration Manager > Select Protocols > IP > VRRP
Default:	1
Options:	1 to 255 seconds
Function:	The interval, in seconds, between the transmission of VRRP advertisements from the primary virtual router.
Instructions:	Enter a value from 1 to 255 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.53.25.1.1.9

Parameter: Critical IP Interface

Path: Configuration Manager > Select Protocols > IP > VRRP

Default: 0.0.0.0 (none)

Options: Any valid IP address in dotted-decimal notation.

Function: Identifies an IP address that determines whether the virtual router assumes the role of the master virtual router and is responsible for forwarding traffic. If the critical IP address is operating, then the virtual router forwards traffic. If the critical IP address is down, then a backup virtual router assumes the responsibilities of the master virtual router and forwards traffic. The critical IP address must be on the same router as the primary IP address.

Instructions: Specify an IP address on the same router where the primary IP address resides.

MIB Object ID: 1.3.6.1.4.1.18.3.5.53.25.1.1.10

Parameter: Token Ring Address

Path: Configuration Manager > Select Protocols > IP > VRRP

Default: None

Options: Use one of the following unused token ring functional addresses:

03-00-02-00-00-00
03-00-04-00-00-00
03-00-08-00-00-00
03-00-10-00-00-00
03-00-20-00-00-00
03-00-40-00-00-00
03-00-80-00-00-00
03-00-00-01-00-00
03-00-00-02-00-00
03-00-00-04-00-00
03-00-00-08-00-00

Function: Identifies the token ring functional address for the virtual router ID MAC address that is configured on an IP interface over token ring.

Instructions: Specify a unique functional token ring address. You must specify a token ring functional address for virtual routers on an IP interface over token ring or VRRP will not function.

MIB Object ID: 1.3.6.1.4.1.18.3.5.53.25.1.1.13

Glossary

advertisement An IP packet periodically broadcast by the master virtual router to prevent any of the backup virtual routers from becoming the master virtual router.

backup virtual router One of a set of VRRP routers available to become the master virtual router. A router may be the master virtual router and/or the backup virtual router for many virtual routers.

critical IP interface A local IP interface associated with a virtual router. When the state of this interface changes, the virtual router switches roles. For example, if you designate IP address 1.1.1.1 as the critical IP address for virtual router 1 on router B, and IP address 1.1.1.1 fails, then virtual router 1 on router B is no longer the master virtual router, and a backup virtual router becomes the master virtual router.

master virtual router The VRRP router that assumes responsibility for forwarding data packets received at the MAC address associated with its virtual router, and answers ARP requests for its IP address. A router may be the master virtual router and/or the backup virtual router for many virtual routers.

primary IP address The real IP interface address used as the source IP address for the IP packets carrying advertisements.

priority The value that determines whether a virtual router serves as the master or backup virtual router. The VRRP router with the highest priority becomes the master virtual router. The value of 255 is reserved for the router that owns the IP address associated with the virtual router. The value of 0 is reserved for the master virtual router to indicate that it is releasing responsibility for the virtual router. The range of 1 to 254 is available for VRRP routers backing up the virtual router. The default priority is 100.

virtual MAC address A unicast MAC address associated with each virtual router and used as the source MAC address for VRRP advertisements. The master virtual router uses this address instead of its physical MAC address in all communication.

virtual router	A software-defined object managed by VRRP that corresponds to an IP address on a LAN segment. A virtual router typically exists on multiple VRRP routers, one of which acts as the master virtual router for this IP address, while the others act as backup virtual routers.
VRID	The virtual router identifier configured in the range of 1 to 255. The VRID must be unique within the subnet.
VRRP router	A router running the Virtual Router Redundancy Protocol. A VRRP router may participate in one or more virtual routers.

Index

A

acronyms, xi
adding a virtual router, 3-3
Advertisement Interval parameter, A-4
advertisement interval, setting, 3-5

B

backup virtual router, defined, 1-2

C

configuring a virtual router, 2-1
conventions, text, x
Critical IP Interface parameter, A-5
critical IP interface, specifying, 3-6

D

disabling a virtual router, 3-2

E

educational services, xii
Enable parameter, A-3
enabling a virtual router, 3-2

I

IP address to be backed up, assigning, 3-3
IP multicast datagrams, 1-2

M

MAC address, 1-2, 2-2
master virtual router, defined, 1-2
messaging, 1-2

P

primary IP address, 2-1
Primary IP Address parameter, A-2
priority of virtual routers, defined, 1-2
Priority parameter, A-4
priority, setting, 3-4
product support, xii
protocol messaging, defined, 1-2
publications, Bay Networks, xi

R

redundancy services, planning, 1-3
router redundancy, characteristics, 1-3

S

support, Bay Networks, xii

T

technical publications, xi
technical support, xii
text conventions, x
Token Ring Address parameter, A-5
token ring address, setting, 3-7
token ring functional address, 3-7

V

virtual router
  configuring, 2-1
  disabling, 3-2
  enabling, 3-2
virtual router ID (VRID), assigning, 2-2
Virtual Router ID parameter, A-2
Virtual Router IP Address parameter, A-2, A-4
virtual router IP address, assigning, 2-2
VRRP advertisements, 3-5